CLAIMS:

1. A computer-implemented method comprising:

determining, from an event store, a compromised account dataset comprising compromised user account examples, each compromised user account example being associated with a user account that has been compromised or has been subjected to an attempted security breach, and comprising a first plurality of event objects;

determining, from the event store, an uncompromised account dataset comprising uncompromised user account examples, each uncompromised user account example being associated with a user account that has not been compromised and has not been subjected to an attempted security breach, and comprising a second plurality of event objects;

determining a training dataset, the training data set comprising a plurality of compromised user account examples from the compromised account dataset and a plurality of uncompromised user account examples from the uncompromised account dataset, wherein one or more of the compromised user account examples comprise a label indicative of a security risk, and one or more of the uncompromised user account examples comprise a label indicative of no security risk;

determining a set of attributes from each of the plurality of compromised user account examples and the plurality of uncompromised user account examples;

determining a numerical representation of each set of attributes, wherein at least some of the numerical representations are associated with the respective label of the compromised or uncompromised user account examples from which the associated set of attributes was determined;

training a compromised account detection model using the numerical representations and the labels to predict a likelihood of a candidate user account being a security risk; and

providing the trained compromised account detection model, wherein the set of attributes comprises a user role type attribute, and the user role type attribute comprises a dual or multi role value.

2. The method of claim 1, wherein user accounts of the user account examples of the compromised account dataset and the uncompromised account dataset are associated with a same user role type attribute.

3. The method of claim 1, wherein user accounts of the user account examples of the compromised account dataset and the uncompromised account dataset are associated with a plurality of different user role type attributes.

4. The method from claim 3, wherein a first feature value of each of the numerical representations of the plurality of compromised user account examples and the plurality of uncompromised user account examples user is a role type attribute value.

5. The computer-implemented method of any one of claims 2 to 4, wherein the set of attributes determined from the uncompromised user account examples are indicative of standard user behaviours for the user role type attribute and the set of attributes determined from the compromised user account examples are indicative of non-standard and/or anomalous user behaviours for the user role type attribute.

6. The computer-implemented method of any one of the preceding claims, wherein the training of the compromised account detection model comprises:

an adaptive sliding window data selection method.

7. The computer-implemented method of claim 6, wherein the adaptive sliding window selection method comprises:

determining one or more account example subsets of the uncompromised account dataset and/or the compromised account dataset; and

determining one or more attribute subsets from each of the plurality of compromised user account examples and each of the plurality of uncompromised user account examples in the one or more account example subsets.

8. The computer-implemented method of claim 6, wherein the adaptive sliding window selection method comprises:

determining one or more attribute subsets of the set of attributes.

9. The computer-implemented method of claims 6 to 8, wherein the one or more attribute subsets are determined based on one or more of: time of day, business hours, user role type and/or periods of high activity.

10. The computer implemented method of any one of claims 7 to 9, wherein the compromised account detection model is trained using the set of attribute subsets.

11. The computer-implemented method of any one of the preceding claims, wherein determining the numerical representation of each set of attributes comprises:

encoding one or more of the attributes into an ordinal encoding, wherein the ordinal encoding is indicative of a sequential relationship between each of the plurality of compromised user account examples and wherein the ordinal encoding is indicative of a sequential relationship between each of the plurality of uncompromised user account examples.

12. The computer implemented method of any one of the previous claims, further comprising:

generating one or more artificial compromised account examples using a generative machine learning model.

13. A computer implemented method comprising:

responsive to receiving a trigger request associated with a user account, determining, from an event log of the user account at an event store, a user account dataset, the user account dataset comprising a plurality of event objects;

determining, from the plurality of event objects, a set of attributes;

determining a numerical representation of the set of attributes;

providing, to a compromised account detection model, the numerical representation, the compromised account detection model configured to predict user account security risks; and

outputting, by the compromised account detection model, an indication of whether the user account is compromised or whether the user account has been subjected to a potential security breach, wherein the set of attributes comprises a user role type attribute, and the user role type attribute comprises a dual or multi role value.

14. The computer-implemented method of claim 13, further comprising:

determining a user role type attribute value associated with the user account; and

selecting the compromised account detection model from a plurality of compromised account detection models based on the user role type attribute value, wherein the selected compromised account detection model is configured to output an indication of whether the user account is compromised or whether the user account has been subjected to a potential security breach specific to the determined user role type attribute.

15. The computer-implemented method of claims 13 or 14, wherein the indication of whether the user account is compromised or whether the user account has been subjected to a potential security breach comprises:

determining that the user account dataset is indicative of user behaviour that is non-standard.

16. The method of any one of claims 13 to 15, wherein the trigger request is one of:

an access credential request;

an automatic compromised account check request; or

a manual compromised account check request

17. The computer implemented method of any one of claims 13 to 16, wherein the compromised account detection model is trained according to the method of any one of claims 1 to 12.

18. The computer implemented method of any one of the preceding claims, wherein the one or more attributes comprise or are indicative of one or more of:

authentication/authorisation request type;

authentication/authorisation request time;

authentication/authorisation request frequency;

authentication/authorisation request originating location;

local time of the authentication/authorisation request originating location;

password strings;

email addresses;

two-factor authentication/authorisation information;

request device identifier;

business hours; and

high network traffic times.

19. A system comprising:

memory having instructions embodied thereon; and

one or more processors configured by the instructions to perform the method of any one of the preceding claims.

20. A non-transitory machine-readable storage medium storing instructions which, when executed by one or more processors, cause the one or more processors to perform the method of any one of claims 1 to 18.